

# Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/005253

International filing date: 23 March 2005 (23.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP  
Number: 2004-085364  
Filing date: 23 March 2004 (23.03.2004)

Date of receipt at the International Bureau: 12 May 2005 (12.05.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland  
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁  
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日  
Date of Application: 2 0 0 4 年 3 月 2 3 日

出 願 番 号  
Application Number: 特 願 2 0 0 4 - 0 8 5 3 6 4

パリ条約による外国への出願  
に用いる優先権の主張の基礎  
となる出願の国コードと出願  
番号  
J P 2 0 0 4 - 0 8 5 3 6 4  
The country code and number  
of your priority application,  
to be used for filing abroad  
under the Paris Convention, is

出 願 人  
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 2 0 日

特許庁長官  
Commissioner,  
Japan Patent Office

小 川



【書類名】	特許願	
【整理番号】	2048160094	
【提出日】	平成16年 3月23日	
【あて先】	特許庁長官 殿	
【国際特許分類】	G09C 1/00	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	井藤 好克	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	宮▲ざき▼ 雅也	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	大森 基司	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	原田 俊治	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	横田 薫	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	中野 稔久	
【発明者】		
【住所又は居所】	大阪府門真市大字門真1006番地	松下電器産業株式会社内
【氏名】	▲たか▼橋 潤	
【特許出願人】		
【識別番号】	000005821	
【氏名又は名称】	松下電器産業株式会社	
【代理人】		
【識別番号】	100090446	
【弁理士】		
【氏名又は名称】	中島 司朗	
【手数料の表示】		
【予納台帳番号】	014823	
【納付金額】	21,000円	
【提出物件の目録】		
【物件名】	特許請求の範囲	1
【物件名】	明細書	1
【物件名】	図面	1
【物件名】	要約書	1
【包括委任状番号】	9003742	

【書類名】 特許請求の範囲

【請求項 1】

コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、

前記端末装置は、第 1 のコンテンツを記憶する記憶部を備え、

前記第 1 のコンテンツを前記可搬媒体に移動する際、前記第 1 のコンテンツの一部である部分情報を消去して、前記第 1 のコンテンツを利用不可状態にして、

前記可搬媒体は、第 2 のコンテンツを記録するコンテンツ記録領域を備え、

前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする著作権保護システム。

【請求項 2】

前記著作権保護システムであって、

前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、

前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第 1 のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする請求項 1 記載の著作権保護システム。

【請求項 3】

前記著作権保護システムであって、

前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、

前記部分情報記録領域に記録した部分情報を前記第 1 のコンテンツに書き戻して利用可能状態にすることを特徴とする請求項 2 記載の著作権保護システム。

【請求項 4】

前記著作権保護システムであって、

前記端末装置の記憶部は、第 1 のコンテンツを 1 つ以上のブロックに分割して記録し、

前記部分情報は、前記ブロックから各々選択することを特徴とする請求項 1 から請求項 3 のいずれか 1 項に記載の著作権保護システム。

【請求項 5】

前記著作権保護システムであって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、

第 1 のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、

前記第 1 のコンテンツを前記可搬媒体に移動する際、

前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第 1 のコンテンツを利用不可状態にすることを特徴とする請求項 1 から請求項 4 のいずれかに記載の著作権保護システム。

【請求項 6】

前記著作権保護システムであって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、

第 1 のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、

前記第 1 のコンテンツを前記可搬媒体に移動する際、

前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、

前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、

前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第 1 のコンテンツを利用不可能状態にすることを特徴とする請求項 1 から請求項 4 のいずれか 1 項に記載の著作権保護システム。

【請求項 7】

前記著作権保護システムであって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、

第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、

前記第１のコンテンツを前記可搬媒体に移動する際、

前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、

前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、

前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１から請求項４のいずれか１項に記載の著作権保護システム。

【請求項８】

前記著作権保護システムであって、

前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、

前記部分情報を前記部分情報記録領域に記録するに際し、

前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする請求項２から請求項７のいずれか１項に記載の著作権保護システム。

【請求項９】

前記著作権保護システムであって、

前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする請求項８に記載の著作権保護システム。

【請求項１０】

コンテンツを保持して、可搬媒体へコンテンツを移動可能な端末装置であって、

前記端末装置は、第１のコンテンツを記憶する記憶部を備え、

前記第１のコンテンツを前記可搬媒体に移動する際、前記第１のコンテンツの一部である部分情報を消去して、前記第１のコンテンツを利用不可状態にして、

前記可搬媒体は、第２のコンテンツを記録するコンテンツ記録領域を備え、

前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする端末装置。

【請求項１１】

前記端末装置であって、

前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、

前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第１のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする請求項１０記載の端末装置。

【請求項１２】

前記端末装置であって、

前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、

前記部分情報記録領域に記録した部分情報を前記第１のコンテンツに書き戻して利用可能状態にすることを特徴とする請求項１１記載の端末装置。

【請求項１３】

前記端末装置であって、

前記端末装置の記憶部は、第１のコンテンツを１つ以上のブロックに分割して記録し、

前記部分情報は、前記ブロックから各々選択することを特徴とする請求項１０から請求項１２のいずれか１項に記載の端末装置。

【請求項１４】

前記端末装置であって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、

第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、

前記第１のコンテンツを前記可搬媒体に移動する際、

前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第１のコンテンツを利用不可状態にすることを特徴とする請求項１０から請求項１３のいずれか１項に記載の端末装置。

【請求項１５】

前記端末装置であって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、

第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、

前記第１のコンテンツを前記可搬媒体に移動する際、

前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、

前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、

前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１０から請求項１３のいずれか１項に記載の端末装置。

【請求項１６】

前記端末装置であって、

前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、

第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、

前記第１のコンテンツを前記可搬媒体に移動する際、

前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、

前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、

前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする請求項１０から請求項１３のいずれか１項に記載の端末装置。

【請求項１７】

前記端末装置であって、

前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、

前記部分情報を前記部分情報記録領域に記録するに際し、

前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする請求項１１から請求項１６のいずれか１項に記載の端末装置。

【請求項１８】

前記端末装置であって、

前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする請求項１７に記載の端末装置。

【書類名】 明細書

【発明の名称】 記録再生装置、可搬媒体、及び著作権保護システム

【技術分野】

【0001】

本発明は、コンテンツの不正利用防止を目的とした記録再生装置、及び可搬媒体を含む著作権保護システムに関し、特に、不正利用を防止しつつユーザの利便性を高める技術に関する。

【背景技術】

【0002】

近年、BSデジタル放送や地上デジタル放送の開始に伴い、映画等のデジタルコンテンツが広く配信されるようになってきている。デジタルコンテンツ（以下、コンテンツ）は複製が容易であるため、インターネットやその他の媒体を介した海賊行為、並びに複製コンテンツの再配信などの不正行為に対する懸念が高まっており、これら不正行為に対抗（コンテンツを保護）するための技術開発が進められている。

【0003】

このようなコンテンツの保護技術に関する規格として、例えば、DTCP（Digital Transmission Content Protection）がある。DTCPは、コンテンツをデジタル転送する際に、コンテンツを暗号化するなどして不正コピーを防止する技術である。DTCPのようなコンテンツ保護技術においては、コンテンツに、「Copy No More」、「Copy One Generation」等のコピー制御情報（CCI：Copy Control Information）を付与する。「Copy No More」はコンテンツのコピーが禁止されていることを表し、「Copy One Generation」はコンテンツのコピーが1回だけ許されていることを表す。従って、コピー制御情報として「Copy One Generation」が付与されたコンテンツをコピーすると、コピーによって新たに得られたコンテンツには、コピー制御情報として「Copy No More」が付与される。

【0004】

一方で、コピー制御情報として「Copy No More」が付与されたコンテンツであっても、他の記録媒体、あるいは他の装置へ移動させたいという要望がある。例えば、デジタルテレビに内蔵されているHDD（Hard Disk Drive）に記録されているコンテンツをDVD-RAMに移動させて保存版として保管しておきたいような場合である。この際（HDDからDVD-RAMにコンテンツを移動させた場合）、デジタルテレビ内蔵HDDの当該コンテンツは、当然、再生できない状態にされなければならない。例えば、内蔵HDDからDVD-RAMにコンテンツをコピーした後に、内蔵HDDに記録されているコンテンツを消去するなどしてコンテンツを無効化する、すなわちコンテンツを利用できない状態にする方法などが考えられる。しかしながら、コンテンツの移動に先立ってデジタルテレビから内蔵HDDを取り出し、これをパーソナルコンピュータに接続してバックアップを作成し、コンテンツを移動した後にバックアップしておいたデータを内蔵HDDに戻すという操作が行われると、コンテンツを何度でも移動できることになり、事実上不正コピーを防止することができなくなる。

【0005】

また、コンテンツの移動中に電源断などの原因により、移動元と移動先のコンテンツが共に損なわれ、コンテンツとして利用できなくなることは、コンテンツを利用するユーザにとっては不便である。さらに、このようにして利用できなくなったコンテンツを再度入手するために出費が必要な場合には経済的な損失も発生する。

上記課題を解決するための従来技術として、不正コピーを防止しながら、コンテンツの喪失を招くことなく、コンテンツの移動を可能にする技術が特許文献1に開示されている。

【特許文献1】 特開2003-228522号公報

【非特許文献1】 「現代暗号理論」、池野信一、小山謙二、電子通信学会

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、移動元のコンテンツが高画質コンテンツであり、コンテンツのサイズに比べて、移動先の記録容量が小さい場合には、コンテンツの移動前に、その画質を劣化させるなどしてサイズを小さく圧縮変換してから移動を行うのが通例であるが、前記構成のようにコンテンツを消去するなどして移動元のコンテンツを無効化する場合、圧縮変換された（画質の劣化した）コンテンツだけがユーザの下に残ることになる。すなわち、再び記録容量の大きな内蔵HDDへコンテンツを戻す（移動する）場合であっても、画質の劣化されたコンテンツを高画質コンテンツへ変換することは不可能であり、元々の高画質コンテンツは復元されないため、これはコンテンツを利用するユーザの利便性が損なわれることにつながる。

【0007】

本発明は、前記課題を解決するものであって、不正コピーを防止しながら、コンテンツの喪失を招くことなくコンテンツの移動を可能にして、さらに、サイズを小さくする圧縮変換後であっても、当該コンテンツを移動元に戻す場合には、元々の高画質コンテンツの復元を可能にする記録再生装置、並びに可搬媒体を含む著作権保護システムの提供を目的とする。

【課題を解決するための手段】

【0008】

本発明は、コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な著作権保護システムであって、前記端末装置は、第1のコンテンツを記憶する記憶部を備え、前記第1のコンテンツを前記可搬媒体に移動する際、前記第1のコンテンツの一部である部分情報を消去して、前記第1のコンテンツを利用不可状態にして、前記可搬媒体は、第2のコンテンツを記録するコンテンツ記録領域を備え、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする。

【0009】

また、本発明は、前記著作権保護システムであって、前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第1のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、前記部分情報記録領域に記録した部分情報を前記第1のコンテンツに書き戻して利用可能状態にすることを特徴とする。

【0010】

また、本発明は、前記著作権保護システムであって、前記端末装置の記憶部は、第1のコンテンツを1つ以上のブロックに分割して記録し、前記部分情報は、前記ブロックから各々選択することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第1のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第1のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第1のコンテンツを利用不可状態にすることを特徴とする。

【0011】

また、本発明は、前記著作権保護システムであって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第1のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第1



のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第1のコンテンツを利用不可能状態にすることを特徴とする。

【0012】

また、本発明は、前記著作権保護システムであって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第1のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第1のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第1のコンテンツを利用不可能状態にすることを特徴とする。

【0013】

また、本発明は、前記著作権保護システムであって、前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、前記部分情報を前記部分情報記録領域に記録するに際し、前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする。

また、本発明は、前記著作権保護システムであって、前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする。

【0014】

また本発明は、コンテンツを保持する端末装置から、可搬媒体へコンテンツを移動可能な端末装置であって、前記端末装置は、第1のコンテンツを記憶する記憶部を備え、前記第1のコンテンツを前記可搬媒体に移動する際、前記第1のコンテンツの一部である部分情報を消去して、前記第1のコンテンツを利用不可状態にして、前記可搬媒体は、第2のコンテンツを記録するコンテンツ記録領域を備え、前記移動するコンテンツを前記コンテンツ記録領域に記録することを特徴とする。

【0015】

また、本発明は、前記端末装置であって、前記可搬媒体は、前記部分情報を記録する部分情報記録領域を備え、前記端末装置は、前記端末装置から前記可搬媒体へコンテンツを移動する際に、前記第1のコンテンツから前記部分情報を消去するに先立ち、前記部分情報を前記部分情報記録領域に記録することを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置は、前記端末装置から前記可搬媒体へ移動したコンテンツを再度前記端末装置へ戻す際に、前記部分情報記録領域に記録した部分情報を前記第1のコンテンツに書き戻して利用可能状態にすることを特徴とする。

【0016】

また、本発明は、前記端末装置であって、前記端末装置の記憶部は、第1のコンテンツを1つ以上のブロックに分割して記録し、前記部分情報は、前記ブロックから各々選択することを特徴とする。

また、本発明は、前記端末装置であって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第1のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第1のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツから前記部分情報を選択して消去して、前記第1のコンテンツを利用不可状態にすることを特徴とする。

【0017】

また、本発明は、前記端末装置であって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第1の

コンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報を選択し、前記復号化したコンテンツの前記部分情報に対応する部分を消去した情報を、前記暗号化部で再度暗号化し、前記記憶部に記憶された暗号化コンテンツを前記再度暗号化した情報で上書きすることで、前記第１のコンテンツを利用不可能状態にすることを特徴とする。

#### 【００１８】

また、本発明は、前記端末装置であって、前記端末装置はコンテンツを暗号化する暗号化部と、前記暗号化部により暗号化されたコンテンツを復号する復号化部を備え、第１のコンテンツは前記暗号化部により暗号化して前記記憶部に記憶され、前記第１のコンテンツを前記可搬媒体に移動する際、前記記憶部に記憶された暗号化コンテンツを前記復号化部で復号化したコンテンツから前記部分情報の位置を選択し、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を部分情報とし、前記記憶部に記憶された暗号化コンテンツの、前記選択した位置に対応する部分を消去することで、前記第１のコンテンツを利用不可能状態にすることを特徴とする。

#### 【００１９】

また、本発明は、前記端末装置であって、前記部分情報を暗号化する部分情報暗号化部と、前記部分情報暗号化部により暗号化された部分情報を復号化する部分情報復号化部を備え、前記部分情報を前記部分情報記録領域に記録するに際し、前記部分情報を前記部分情報暗号化部により暗号化して記録することを特徴とする。

また、本発明は、前記端末装置であって、前記部分情報を暗号化もしくは復号化する鍵は、コンテンツの暗号化に用いる鍵と同じであることを特徴とする。

#### 【発明の効果】

#### 【００２０】

本発明によれば、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツの部分情報を移動させることにより、記録再生装置内のコンテンツをすべて消去することなく利用不可状態にし、移動したコンテンツを再び当該記録再生装置へ戻す場合には、前記部分情報を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にすることが可能となる。

#### 【発明を実施するための最良の形態】

#### 【００２１】

以下、本発明の実施の形態について、図面を参照しながら説明する。図１は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツを供給するコンテンツ供給装置１０１と、前記コンテンツを獲得して、コンテンツの記録、並びに再生を行い、さらにコンテンツの移動を実行する記録再生装置１０２と、前記移動するコンテンツを獲得する記録再生装置１０３、あるいは可搬媒体１０４からなる。

#### 【００２２】

記録再生装置１０２は、コンテンツ供給装置１０１からコンテンツを受信して記録する際、当該コンテンツを暗号化して、例えば内蔵ＨＤＤに記録する。そして、当該コンテンツを移動する際は、移動先となる装置、あるいは可搬媒体が正規装置、あるいは正規可搬媒体であるか否かを確認（認証）した上で、コンテンツの移動を実行する。さらに、記録再生装置１０２は、コンテンツの移動が完了した後に、内部に記録するコンテンツを利用できない状態にする。ここで、認証技術は、例えばＤＴＣＰ規格で定められた手順に従う、あるいは非特許文献１、並びに非特許文献２に開示される公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。

#### 【００２３】

##### （実施の形態１）

図２は、本発明の実施の形態１における、記録再生装置１０２が可搬媒体１０４にコンテンツを移動させる場合の記録再生装置１０２、並びに可搬媒体１０４の機能を示す機能ブロック図である。

記録再生装置 102 は、外部からのコンテンツを受信するコンテンツ受信部 201 と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部 202 と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部 203 と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部 204 と、暗号化コンテンツ記録部 204 に記録された前記暗号化したコンテンツを読み出す暗号化コンテンツ読出し部 205 と、前記装置記録鍵を用いて、暗号化コンテンツ読出し部 205 が読み出した前記暗号化したコンテンツを復号する復号部 206 と、前記復号したコンテンツを（圧縮）変換する変換部 207 と、変換部 207 が変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部 208 と、前記媒体記録鍵を記憶する媒体記録鍵記憶部 209 と、前記媒体記録鍵を用いて、変換部 207 が変換したコンテンツを暗号化する暗号化部 210 と、暗号化コンテンツ読出し部 205 が読み出した前記暗号化したコンテンツから部分情報を選択する部分情報選択部 211 と、前記部分情報を記憶する部分情報記憶部 212 と、部分情報記憶部 212 に記憶された前記部分情報に対応して暗号化コンテンツ記録部 204 に書き込みを行う部分情報書込部 213 と、前記暗号化したコンテンツ、前記媒体記録鍵、並びに前記部分情報を可搬媒体 104 に書き込む、あるいは可搬媒体 104 から読み出す書込／読出部 214 とを備える。媒体記録鍵記憶部 209 に記憶する鍵データは、書込／読出部 214 を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

#### 【0024】

また、可搬媒体 104 は、暗号化コンテンツを記録する暗号化コンテンツ領域 221 と、媒体記録鍵を記録する媒体記録鍵領域 222 と、部分情報を記録する部分情報領域 223 を備える。可搬媒体 104 が備える媒体記録鍵領域 222 は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

#### 【0025】

図 3 は暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図である。暗号化コンテンツは 1 つ以上のブロック（EC1 [1]、EC1 [2]、・・・、EC1 [N]）に分けて記録され、各ブロックは装置記録鍵を用いて暗号化されている。

次に、図 4 および図 5 を用いて、記録再生装置 102 から、可搬媒体 104 へコンテンツを移動する場合の動作について説明する。

#### 【0026】

S401：記録再生装置 102 は、媒体記録鍵生成部 208 において媒体記録鍵 K2 を生成して、媒体記録鍵記憶部 209 に、前記生成した媒体記録鍵を記憶する。

S402：記録再生装置 102 は、書込／読出部 214 を介して媒体記録鍵 K2 を媒体記録鍵領域 222 に書き出す。

S403：記録再生装置 102 は、暗号化コンテンツ読出し部 205 において暗号化コンテンツ記録部 204 に記録する暗号化コンテンツの先頭ブロック EC1 [i]（ $i=1$ ）を読み出す。

#### 【0027】

S404：記録再生装置 102 は、暗号化コンテンツのブロックの読み出しに失敗したら S406 に処理を分岐する。そうでなければ、S500 に処理を分岐する。

S500：読み出した暗号化コンテンツのブロックを可搬媒体に移動する。

S405：記録再生装置 102 は、暗号化コンテンツ読出し部 205 において暗号化コンテンツ記録部 204 に記録する暗号化コンテンツの次ブロック EC1 [i]（ $i=i+1$ ）を読み出す。

#### 【0028】

S406：記録再生装置 102 は、媒体記録鍵記憶部 209 に記録された媒体記録鍵 K2 を消去する。

以下のステップは、S500 を詳細化したものである。

S501：記録再生装置 102 は、暗号化コンテンツの 1 ブロック EC1 [i] を復号

部 2 0 6 において、装置記録鍵記憶部 2 0 2 に記憶する装置記録鍵 K 1 を用いて復号し、C 1 [ i ] を生成する。

【 0 0 2 9 】

S 5 0 2 : 記録再生装置 1 0 2 は、変換部 2 0 7 において、S 5 0 1 で復号したブロック C 1 [ i ] を（圧縮）変換し、C 2 [ i ] を生成する。

S 5 0 3 : 記録再生装置 1 0 2 は、暗号化部 2 1 0 において、S 4 0 1 で生成／記憶した媒体記録鍵 K 2 を用いて、S 5 0 2 で変換したコンテンツ C 2 [ i ] を暗号化し、E C 2 [ i ] を生成する。

【 0 0 3 0 】

S 5 0 4 : 記録再生装置 1 0 2 は、S 5 0 3 で暗号化したコンテンツ E C 2 [ i ] を、書込／読出部 2 1 4 を介して可搬媒体 1 0 4 の暗号化コンテンツ領域 2 2 1 へ記録する。

S 5 0 5 : 記録再生装置 1 0 2 は、部分情報選択部 2 1 1 において、暗号化コンテンツの 1 ブロック E C 1 [ i ] から、部分情報 P E C 1 [ i ] を選択（例えば、ブロックの先頭から 5 1 2 b y t e を選択）し、部分情報記憶部 2 1 2 へ記録する。

【 0 0 3 1 】

S 5 0 6 : 記録再生装置 1 0 2 は、暗号化コンテンツ記録部 2 0 4 に記録された暗号化コンテンツの、部分情報記憶部 2 1 2 へ記録された P E C 1 [ i ] に対応する部分を無意味な情報（例えば全て 0 ）で上書きする。

S 5 0 7 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 に記憶する部分情報 P E C 1 [ i ] を、書込／読出部 2 1 4 を介して可搬媒体 1 0 4 の部分情報領域 2 2 3 へ記録する。

【 0 0 3 2 】

S 5 0 8 : 記録再生装置 1 0 2 は装置内の、部分情報記憶部 2 1 2 に記憶する部分情報 P E C 1 [ i ] と、S 5 0 1 で生成した C 1 [ i ] と、S 5 0 2 で生成した C 2 [ i ] と、S 5 0 3 で生成した E C 2 [ i ] を消去する。

図 6 は、記録再生装置 1 0 2 から可搬媒体 1 0 4 へのコンテンツの移動が完了したときの、可搬媒体 1 0 4 の記録状態を示した図である。

【 0 0 3 3 】

次に、図 7 を用いて、可搬媒体 1 0 4 から、記録再生装置 1 0 2 へコンテンツを移動する場合の動作について説明する。

S 7 0 1 : 可搬媒体 1 0 4 は、暗号化コンテンツ領域 2 2 1 に記録する暗号化コンテンツ E C 2 [ i ] （ i = 1 ~ N ）、並びに媒体記録鍵領域 2 2 2 に記録する媒体記録鍵 K 2 を消去する。

【 0 0 3 4 】

S 7 0 2 : 記録再生装置 1 0 2 は、可搬媒体 1 0 4 の部分情報領域 2 2 3 に記録する部分情報の先頭ブロック P E C 1 [ i ] （ i = 1 ）を書込／読出部 2 1 4 を介して読み出す。

S 7 0 3 : 記録再生装置 1 0 2 は、部分情報のブロックの読み出しに失敗したら処理を終了する。そうでなければ、S 7 0 4 に処理を分岐する。

【 0 0 3 5 】

S 7 0 4 : 記録再生装置 1 0 2 は、読出した部分情報 P E C 1 [ i ] を部分情報記憶部 2 1 2 へ記録する。

S 7 0 5 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 へ記録された P E C 1 [ i ] を、暗号化コンテンツ記録部 2 0 4 に記録された暗号化コンテンツの対応する部分へ上書きする。

【 0 0 3 6 】

S 7 0 6 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 と部分情報領域 2 2 3 に記憶する部分情報 P E C 1 [ i ] を消去する。

S 7 0 7 : 記録再生装置 1 0 2 は、可搬媒体 1 0 4 の部分情報領域 2 2 3 に記録する部分情報の次ブロック P E C 1 [ i ] （ i = i + 1 ）を書込／読出部 2 1 4 を介して読み出

す。

### 【0037】

（実施の形態2）

図8は、本発明の実施の形態2における、記録再生装置102が可搬媒体104にコンテンツを移動させる場合の記録再生装置102、並びに可搬媒体104の機能を示す機能ブロック図である。

記録再生装置102は、外部からのコンテンツを受信するコンテンツ受信部201と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部202と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部203と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部204と、暗号化コンテンツ記録部204に記録された前記暗号化したコンテンツを読み出す暗号化コンテンツ読出し部205と、前記装置記録鍵を用いて、暗号化コンテンツ読出し部205が読み出した前記暗号化したコンテンツを復号する復号部206と、復号部206が復号したコンテンツを（圧縮）変換する変換部207と、変換部207が変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部208と、前記媒体記録鍵を記憶する媒体記録鍵記憶部209と、前記媒体記録鍵を用いて、変換部207が変換したコンテンツを暗号化する暗号化部210と、復号部206が復号したコンテンツから部分情報を選択する部分情報選択部211と、前記部分情報を記憶する部分情報記憶部212と、部分情報記憶部212に記憶された前記部分情報に対応して、復号部206が復号した前記復号したコンテンツを加工し、暗号化部203で前記装置記録鍵を用いて暗号化し、暗号化コンテンツ記録部204に書込みを行う部分情報書込部213と、媒体記録鍵記憶部209に記録された前記媒体記録鍵を用いて前記部分情報を暗号化もしくは復号化を行う暗復号化部801と、暗号化部210が暗号化したコンテンツ、前記媒体記録鍵、並びに暗復号化部801が暗号化した部分情報を可搬媒体104に書き込む、あるいは可搬媒体104から読み出す書込／読出部214とを備える。媒体記録鍵記憶部209に記憶する鍵データは、書込／読出部214を介して当該鍵データが媒体に書き込まれた後は、そのデータが消去される。

### 【0038】

また、可搬媒体104は、暗号化コンテンツを記録する暗号化コンテンツ領域221と、媒体記録鍵を記録する媒体記録鍵領域222と、部分情報を記録する部分情報領域223を備える。可搬媒体104が備える媒体記録鍵領域222は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

### 【0039】

図3は暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図である。暗号化コンテンツは1つ以上のブロック（EC1[1]、EC1[2]、・・・、EC1[N]）に分けて記録され、各ブロックは装置記録鍵を用いて暗号化されている。

次に、図4および図9を用いて、記録再生装置102から、可搬媒体104へコンテンツを移動する場合の動作について説明する。

### 【0040】

S401：記録再生装置102は、媒体記録鍵生成部208において媒体記録鍵K2を生成して、媒体記録鍵記憶部209に、前記生成した媒体記録鍵を記憶する。

S402：記録再生装置102は、書込／読出部214を介して媒体記録鍵K2を媒体記録鍵領域223に書き出す。

S403：記録再生装置102は、暗号化コンテンツ読出し部205において暗号化コンテンツ記録部204に記録する暗号化コンテンツの先頭ブロックEC1[i]（i=1）を読み出す。

### 【0041】

S404：記録再生装置102は、暗号化コンテンツのブロックの読み出しに失敗したらS406に処理を分岐する。そうでなければ、S500に処理を分岐する。

S 5 0 0 : 読み出した暗号化コンテンツのブロックを可搬媒体に移動する。

S 4 0 5 : 記録再生装置 1 0 2 は、暗号化コンテンツ読出し部 2 0 5 において暗号化コンテンツ記録部 2 0 4 に記録する暗号化コンテンツの次ブロック E C 1 [ i ] ( i = i + 1 ) を読み出す。

【 0 0 4 2 】

S 4 0 6 : 記録再生装置 1 0 2 は、媒体記録鍵記憶部 2 0 9 に記録された媒体記録鍵 K 2 を消去する。

以下のステップは、S 5 0 0 を詳細化したものである。

S 9 0 1 : 記録再生装置 1 0 2 は、暗号化コンテンツの 1 ブロック E C 1 [ i ] を復号部 2 0 6 において、装置記録鍵記憶部 2 0 2 に記憶する装置記録鍵 K 1 を用いて復号し、C 1 [ i ] を生成する。

【 0 0 4 3 】

S 9 0 2 : 記録再生装置 1 0 2 は、変換部 2 0 7 において、S 9 0 1 で復号したブロック C 1 [ i ] を(圧縮)変換し、C 2 [ i ] を生成する。

S 9 0 3 : 記録再生装置 1 0 2 は、暗号化部 2 1 0 において、S 4 0 1 で生成／記憶した媒体記録鍵 K 2 を用いて、S 9 0 2 で変換したコンテンツ C 2 [ i ] を暗号化し、E C 2 [ i ] を生成する。

【 0 0 4 4 】

S 9 0 4 : 記録再生装置 1 0 2 は、S 9 0 3 で暗号化したコンテンツ E C 2 [ i ] を、書込／読出部 2 1 4 を介して可搬媒体 1 0 4 の暗号化コンテンツ領域 2 2 1 へ記録する。

S 9 0 5 : 記録再生装置 1 0 2 は、部分情報選択部 2 1 1 において、S 9 0 1 で復号化した C 1 [ i ] から、部分情報 P C 1 [ i ] を選択(例えば、ブロックの構成を示すタグ情報部分を選択)し、部分情報記憶部 2 1 2 へ記録する。

【 0 0 4 5 】

S 9 0 6 : 記録再生装置 1 0 2 は、S 9 0 1 で復号化した C 1 [ i ] において部分情報 P C 1 [ i ] として選択した部分を無意味な情報(例えば全て 0)に変更し、さらに暗号化部 2 0 3 で装置記録鍵 K 1 を暗号化鍵として暗号化したもので、暗号化コンテンツ記録部 2 0 4 に記録された暗号化コンテンツの 1 ブロック E C 1 [ i ] に対応する部分を上書きする。

【 0 0 4 6 】

S 9 0 7 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 に記憶する部分情報 P C 1 [ i ] を暗復号化部 8 0 1 で媒体記録鍵 K 2 を用いて暗号化して E P C 1 [ i ] とし、書込／読出部 2 1 4 を介して可搬媒体 1 0 4 の部分情報領域 2 2 3 へ記録する。

S 9 0 8 : 記録再生装置 1 0 2 は装置内の、部分情報記憶部 2 1 2 に記憶する部分情報 P C 1 [ i ] と、S 9 0 1 で生成した C 1 [ i ] と、S 9 0 2 で生成した C 2 [ i ] と、S 9 0 3 で生成した E C 2 [ i ] と、S 9 0 7 で生成した E P C 2 [ i ] を消去する。

【 0 0 4 7 】

図 1 0 は、記録再生装置 1 0 2 から可搬媒体 1 0 4 へのコンテンツの移動が完了したときの、可搬媒体 1 0 4 の記録状態を示した図である。

次に、図 1 1 を用いて、可搬媒体 1 0 4 から、記録再生装置 1 0 2 へコンテンツを移動する場合の動作について説明する。

S 1 1 0 1 : 記録再生装置 1 0 2 は、可搬媒体 1 0 4 の装置記録鍵領域 2 2 2 に記録する媒体記録鍵 K 2 を書込／読出部 2 1 4 を介して読み出し、媒体記録鍵記憶部 2 0 9 に記録する。

【 0 0 4 8 】

S 1 1 0 2 : 可搬媒体 1 0 4 は、暗号化コンテンツ領域 2 2 1 に記録する暗号化コンテンツ E C 2 [ i ] ( i = 1 ~ N )、並びに媒体記録鍵領域 2 2 2 に記録する媒体記録鍵 K 2 を消去する。

S 1 1 0 3 : 記録再生装置 1 0 2 は、暗号化コンテンツ読出し部 2 0 5 において暗号化コンテンツ記録部 2 0 4 に記録する暗号化コンテンツの先頭ブロック E C 1 [ i ] ( i =

1) を暗号化コンテンツ読出し部 205 を介して読出し、さらに可搬媒体 104 の部分情報領域 223 に記録する部分情報の先頭ブロック EPC1[i] ( $i=1$ ) を書込／読出部 214 を介して読み出す。

#### 【0049】

S1104：記録再生装置 102 は、暗号化コンテンツのブロック及び部分情報のブロックの読み出しに失敗したら S1110 に処理を分岐する。そうでなければ、S1105 に処理を分岐する。

S1105：記録再生装置 102 は、暗号化コンテンツの 1 ブロック EC1[i] を復号部 206 において、装置記録鍵記憶部 202 に記憶する装置記録鍵 K1 を用いて復号し、C1[i] を生成する。

#### 【0050】

S1106：記録再生装置 102 は、読出した部分情報 EPC1[i] を暗復号化部 801 において、媒体記録鍵記憶部 209 に記憶する媒体記録鍵 K2 を用いて復号し、PC1[i] として部分情報記憶部 212 へ記録する。

S1107：記録再生装置 102 は、S1105 で生成した C1[i] に対し、部分情報記憶部 212 へ記録された PC1[i] の相当する箇所を PC1[i] で上書きし、さらに暗号化部 203 で装置記録鍵 K1 を暗号化鍵として暗号化したもので、暗号化コンテンツ記録部 204 に記録された暗号化コンテンツの 1 ブロック EC1[i] に対応する部分を上書きする。

#### 【0051】

S1108：記録再生装置 102 は装置内の、部分情報記憶部 212 に記憶する部分情報 PC1[i] と、S1105 で生成した C1[i] と、さらに部分情報領域 223 の部分情報 EPC1[i] を消去する。

S1109：記録再生装置 102 は、暗号化コンテンツ読出し部 205 において暗号化コンテンツ記録部 204 に記録する暗号化コンテンツの次ブロック EC1[i] ( $i=i+1$ ) を読出し、さらに可搬媒体 104 の部分情報領域 223 に記録する部分情報の次ブロック PEC1[i] ( $i=i+1$ ) を書込／読出部 214 を介して読み出す。

#### 【0052】

S1110：記録再生装置 102 は、媒体記録鍵記憶部 209 に記録された媒体記録鍵 K2 を消去する。

(実施の形態 3)

図 12 は、本発明の実施の形態 3 における、記録再生装置 102 が可搬媒体 104 にコンテンツを移動させる場合の記録再生装置 102、並びに可搬媒体 104 の機能を示す機能ブロック図である。

#### 【0053】

記録再生装置 102 は、外部からのコンテンツを受信するコンテンツ受信部 201 と、前記受信したコンテンツを暗号化するために用いる装置記録鍵を記憶する装置記録鍵記憶部 202 と、前記装置記録鍵を用いて、前記受信したコンテンツを暗号化する暗号化部 203 と、前記暗号化したコンテンツを記録する暗号化コンテンツ記録部 204 と、暗号化コンテンツ記録部 204 に記録された前記暗号化したコンテンツを読み出す暗号化コンテンツ読出し部 205 と、前記装置記録鍵を用いて、暗号化コンテンツ読出し部 205 が読み出した前記暗号化したコンテンツを復号する復号部 206 と、前記復号したコンテンツを(圧縮)変換する変換部 207 と、変換部 207 が変換したコンテンツを暗号化するために用いる媒体記録鍵を生成する媒体記録鍵生成部 208 と、前記媒体記録鍵を記憶する媒体記録鍵記憶部 209 と、前記媒体記録鍵を用いて、変換部 207 が変換したコンテンツを暗号化する暗号化部 210 と、復号部 206 が復号したコンテンツから部分情報として選択する箇所を決定し、暗号化コンテンツ読出し部 205 が読み出した前記暗号化したコンテンツから前記選択箇所の部分情報を抽出する部分情報選択部 211 と、前記部分情報を記憶する部分情報記憶部 212 と、部分情報記憶部 212 に記憶された前記部分情報に対応して暗号化コンテンツ記録部 204 に書込みを行う部分情報書込部 213 と、前記

暗号化したコンテンツ、前記媒体記録鍵、並びに前記部分情報を可搬媒体104に書き込む、あるいは可搬媒体104から読み出す書込／読出部214とを備える。媒体記録鍵記憶部209に記憶する鍵データは、書込／読出部214を介して当該鍵データが可搬媒体104に書き込まれた後は、そのデータが消去される。

#### 【0054】

また、可搬媒体104は、暗号化コンテンツを記録する暗号化コンテンツ領域221と、媒体記録鍵を記録する媒体記録鍵領域222と、部分情報を記録する部分情報領域223を備える。可搬媒体104が備える媒体記録鍵領域222は、鍵を記録するための安全な領域であり、例えば、可搬媒体との認証をパスした装置のみがデータの読み書き可能となるような領域である。

#### 【0055】

図3は暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図である。暗号化コンテンツは1つ以上のブロックに（EC1[1]、EC1[2]、・・・、EC1[N]）分けて記録され、各ブロックは装置記録鍵を用いて暗号化されている。

次に、図4および図13を用いて、記録再生装置102から、可搬媒体104へコンテンツを移動する場合の動作について説明する。

#### 【0056】

S401：記録再生装置102は、媒体記録鍵生成部208において媒体記録鍵K2を生成して、媒体記録鍵記憶部209に、前記生成した媒体記録鍵を記憶する。

S402：記録再生装置102は、書込／読出部214において媒体記録鍵K2を媒体記録鍵領域222に書き出す。

S403：記録再生装置102は、暗号化コンテンツ読出し部205において暗号化コンテンツ記録部204に記録する暗号化コンテンツの先頭ブロックEC1[i]（i=1）を読み出す。

#### 【0057】

S404：記録再生装置102は、暗号化コンテンツのブロックの読み出しに失敗したらS406に処理を分岐する。そうでなければ、S500に処理を分岐する。

S500：読み出した暗号化コンテンツのブロックを可搬媒体に移動する。

S405：記録再生装置102は、暗号化コンテンツ読出し部205において暗号化コンテンツ記録部204に記録する暗号化コンテンツの次ブロックEC1[i]（i=i+1）を読み出す。

#### 【0058】

S406：記録再生装置102は、媒体記録鍵記憶部209に記録された媒体記録鍵K2を消去する。

以下のステップは、S500を詳細化したものである。

S1301：記録再生装置102は、暗号化コンテンツの1ブロックEC1[i]を復号部206において、装置記録鍵記憶部202に記憶する装置記録鍵K1を用いて復号し、C1[i]を生成する。

#### 【0059】

S1302：記録再生装置102は、変換部207において、S1301で復号したブロックC1[i]を（圧縮）変換し、C2[i]を生成する。

S1303：記録再生装置102は、暗号化部210において、S401で生成／記憶した媒体記録鍵K2を用いて、S1302で変換したコンテンツC2[i]を暗号化し、EC2[i]を生成する。

#### 【0060】

S1304：記録再生装置102は、S1303で暗号化したコンテンツEC2[i]を、書込／読出部214を介して可搬媒体104の暗号化コンテンツ領域221へ記録する。

S1305：記録再生装置102は、部分情報選択部211において、暗号化コンテンツの1ブロックEC1[i]から部分情報として選択する箇所を決定し、暗号化コンテン



ツ E C 1 [ i ] の該当箇所から部分情報 P E C 1 [ i ] を選択（例えば、ブロックの先頭から 6 4 b y t e と 5 1 2 b y t e 目から 6 4 b y t e などのように選択）し、位置情報と共に部分情報記憶部 2 1 2 へ記録する。

【 0 0 6 1 】

S 1 3 0 6 : 記録再生装置 1 0 2 は、暗号化コンテンツ記録部 2 0 4 に記録された暗号化コンテンツの、部分情報記憶部 2 1 2 へ記録された P E C 1 [ i ] に対応する部分を無意味な情報（例えば全て 0 ）で上書きする。

S 1 3 0 7 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 に記憶する部分情報 P E C 1 [ i ] を、書込／読出部 2 1 4 を介して可搬媒体 1 0 4 の部分情報領域 2 2 3 へ位置情報と共に記録する。

【 0 0 6 2 】

S 1 3 0 8 : 記録再生装置 1 0 2 は装置内の、部分情報記憶部 2 1 2 に記憶する部分情報 P E C 1 [ i ] と、S 1 3 0 1 で生成した C 1 [ i ] と、S 1 3 0 2 で生成した C 2 [ i ] と、S 1 3 0 3 で生成した E C 2 [ i ] を消去する。

図 6 は、記録再生装置 1 0 2 から可搬媒体 1 0 4 へのコンテンツの移動が完了したときの、可搬媒体 1 0 4 の記録状態を示した図である。

【 0 0 6 3 】

次に、図 7 を用いて、可搬媒体 1 0 4 から、記録再生装置 1 0 2 へコンテンツを移動する場合の動作について説明する。

S 7 0 1 : 可搬媒体 1 0 4 は、暗号化コンテンツ領域 2 2 1 に記録する暗号化コンテンツ E C 2 [ i ] ( i = 1 ~ N ) 、並びに媒体記録鍵領域 2 2 2 に記録する媒体記録鍵 K 2 を消去する。

【 0 0 6 4 】

S 7 0 2 : 記録再生装置 1 0 2 は、可搬媒体 1 0 4 の装置記録鍵領域 2 2 3 に記録する部分情報の先頭ブロック P E C 1 [ i ] ( i = 1 ) を書込／読出部 2 1 4 を介して位置情報と共に読み出す。

S 7 0 3 : 記録再生装置 1 0 2 は、部分情報のブロックの読み出しに失敗したら処理を終了する。そうでなければ、S 7 0 4 に処理を分岐する。

【 0 0 6 5 】

S 7 0 4 : 記録再生装置 1 0 2 は、読出した部分情報 P E C 1 [ i ] を部分情報記憶部 2 1 2 へ記録する。

S 7 0 5 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 へ記録された P E C 1 [ i ] を、暗号化コンテンツ記録部 2 0 4 に記録された暗号化コンテンツの対応する部分へ上書きする。

【 0 0 6 6 】

S 7 0 6 : 記録再生装置 1 0 2 は、部分情報記憶部 2 1 2 と部分情報領域 2 2 3 に記憶する部分情報 P E C 1 [ i ] を消去する。

S 7 0 7 : 記録再生装置 1 0 2 は、可搬媒体 1 0 4 の部分情報領域 2 2 3 に記録する部分情報の次ブロック P E C 1 [ i ] ( i = i + 1 ) を書込／読出部 2 1 4 を介して読み出す。

【 0 0 6 7 】

（その他の変形例）

（１）本発明の実施の形態では、記録再生装置から可搬媒体へコンテンツを移動する、あるいは可搬媒体から記録再生装置へコンテンツを移動する構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置から、別の記録再生装置へコンテンツを移動する構成であってもよい。

【 0 0 6 8 】

（２）本発明の実施の形態では、可搬媒体から記録再生装置へコンテンツを移動する際、可搬媒体に記録する各種データを消去する構成としたが、本発明はその構成に限定されるものではない。例えば、可搬媒体に記録する暗号化コンテンツは消去せずに、復号に必

要な鍵だけを消去して、前記暗号化コンテンツを利用不可状態にする構成であってもよい。また、データの消去ではなく、データの一部を破壊して利用できない状態にする構成であってもよい。

#### 【0069】

(3) 本発明の実施の形態において、記録再生装置が、コンテンツの移動処理における状態遷移を記憶する記憶部を備える構成であってもよい。記録再生装置は、コンテンツの移動が正しく完了しなかった場合、前記記憶部に記憶する状態遷移に基づいて、コンテンツの移動処理を続けて行うか、コンテンツの移動処理を最初からやり直すかを判断する構成であってもよい。さらに、記録再生装置は、前記記憶部に記憶する状態遷移を利用者に通知する通知部を備える構成であってもよい。その場合、正しく完了しなかった旨を利用者に通知して、利用者からの指示に基づいて、コンテンツの移動処理を続けるか、あるいはコンテンツの移動処理を最初からやり直すかを決定する構成であってもよい。

#### 【0070】

(4) 本発明の実施の形態において、記録再生装置、並びに可搬媒体が、鍵を移動後に消去する場合、鍵の受信側が、鍵の送信側に対して正しく受信できたことを通知して、送信側は前記通知に基づいて受信を確認した後に、鍵を消去する構成であってもよい。

(5) 本発明の実施の形態において、コンテンツには当該コンテンツを一意に識別するための識別子が付与されており、可搬媒体に移動させたコンテンツを元の記録再生装置に戻す場合、前記記録再生装置は、自身が保持する暗号化コンテンツの識別子、並びに可搬媒体に記録する暗号化コンテンツの識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。また、コンテンツには、コンテンツを一意に識別する識別子の代わりに、移動元の記録再生装置を一意に識別する識別子が付与されている構成であってもよい。この場合、記録再生装置は、コンテンツに付与されている記録再生装置の識別子と、自身の識別子が一致するか否かを判定して、一致した場合に限り、コンテンツを記録再生装置に移動させることを許可する構成であってもよい。

#### 【0071】

(6) 本発明の実施の形態2では、部分情報を媒体記録鍵で暗号化して可搬媒体に記録する構成としたが、本発明はその構成に限定されるものではない。装置固有鍵で暗号化して記録する構成であってもよいし、別の鍵を新たに生成して暗号化して記録する構成であってもよい。

(7) 本発明の実施の形態では、コンテンツは外部のコンテンツ供給装置により供給される構成としたが、本発明はその構成に限定されるものではない。例えば、記録再生装置に挿入された記録媒体からコンテンツを読み出す構成であってもよい。

#### 【産業上の利用可能性】

#### 【0072】

本発明にかかる著作権保護システムは、コンテンツの移動元の記録再生装置が、コンテンツの移動時に当該コンテンツの部分情報も合わせて移動させることにより、記録再生装置内のコンテンツの全てを消去することなく利用不可状態にすることで、移動したコンテンツを再び当該記録再生装置へ戻す場合に、前記部分情報を元に戻す（移動させる）ことにより、元々の高画質コンテンツを復元可能（利用可能）にできるという効果を有し、ユーザ利便性を損なわない著作権保護システムの実現において有用である。

#### 【図面の簡単な説明】

#### 【0073】

【図1】 本発明に係る著作権保護システムの全体構成を示すブロック図

【図2】 本発明の第1の実施の形態における機能ブロック図

【図3】 本発明の第1、第2及び第3の実施の形態における暗号化コンテンツ記録部に記録された暗号化コンテンツを示す図

【図4】 本発明の第1、第2及び第3の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のメインフロー

【図 5】本発明の第 1 の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のサブルーチン

【図 6】本発明の第 1 及び第 3 の実施の形態における部分情報領域に記録された部分情報を示す図

【図 7】本発明の第 1 及び第 3 の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー

【図 8】本発明の第 2 の実施の形態における機能ブロック図

【図 9】本発明の第 2 の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のサブルーチン

【図 10】本発明の第 2 の実施の形態における部分情報領域に記録された部分情報を示す図

【図 11】本発明の第 2 の実施の形態における可搬媒体から記録再生装置へコンテンツを移動させる際の動作フロー

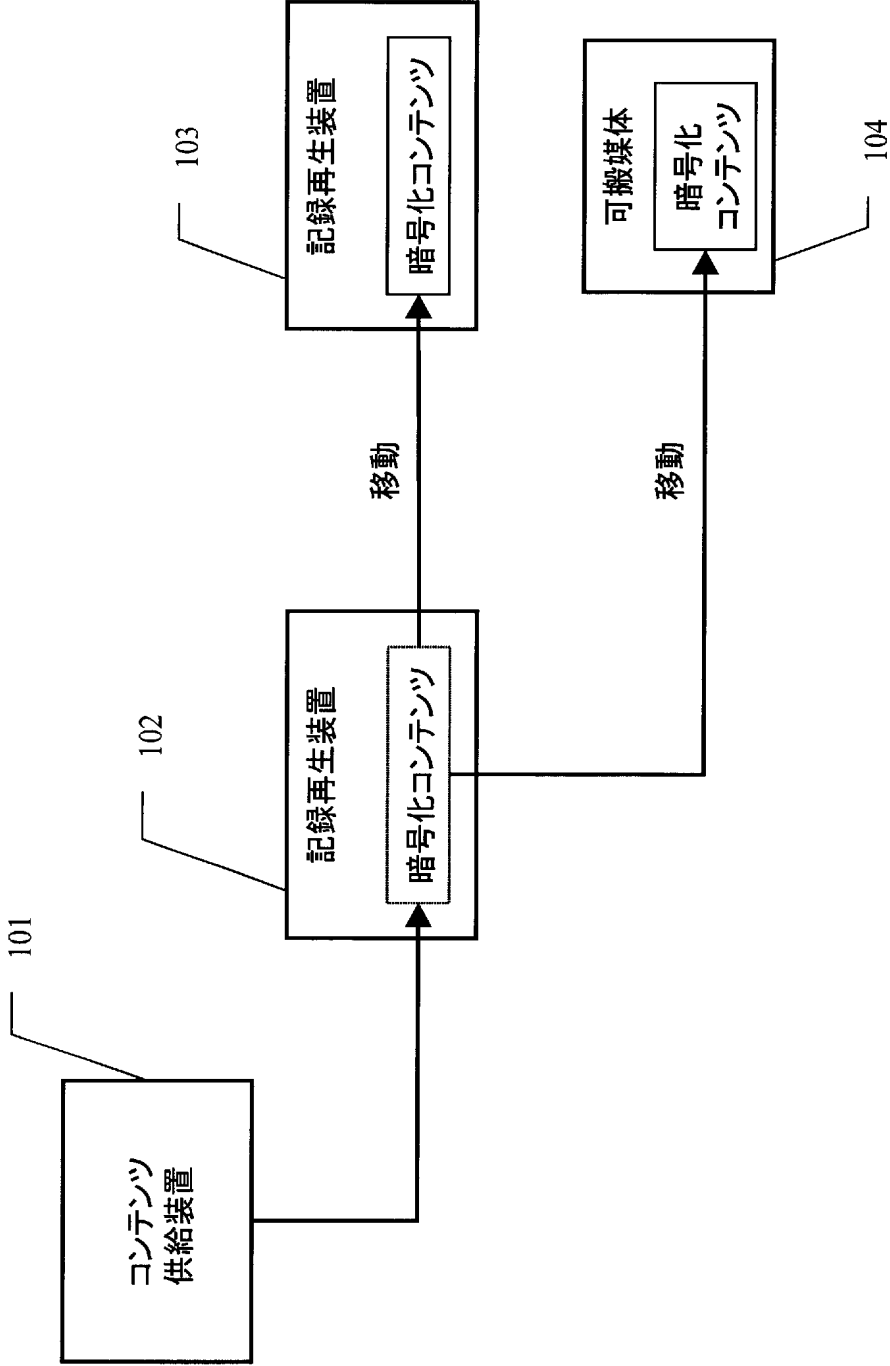
【図 12】本発明の第 3 の実施の形態における機能ブロック図

【図 13】本発明の第 3 の実施の形態における記録再生装置から可搬媒体へコンテンツを移動させる際の動作のサブルーチン

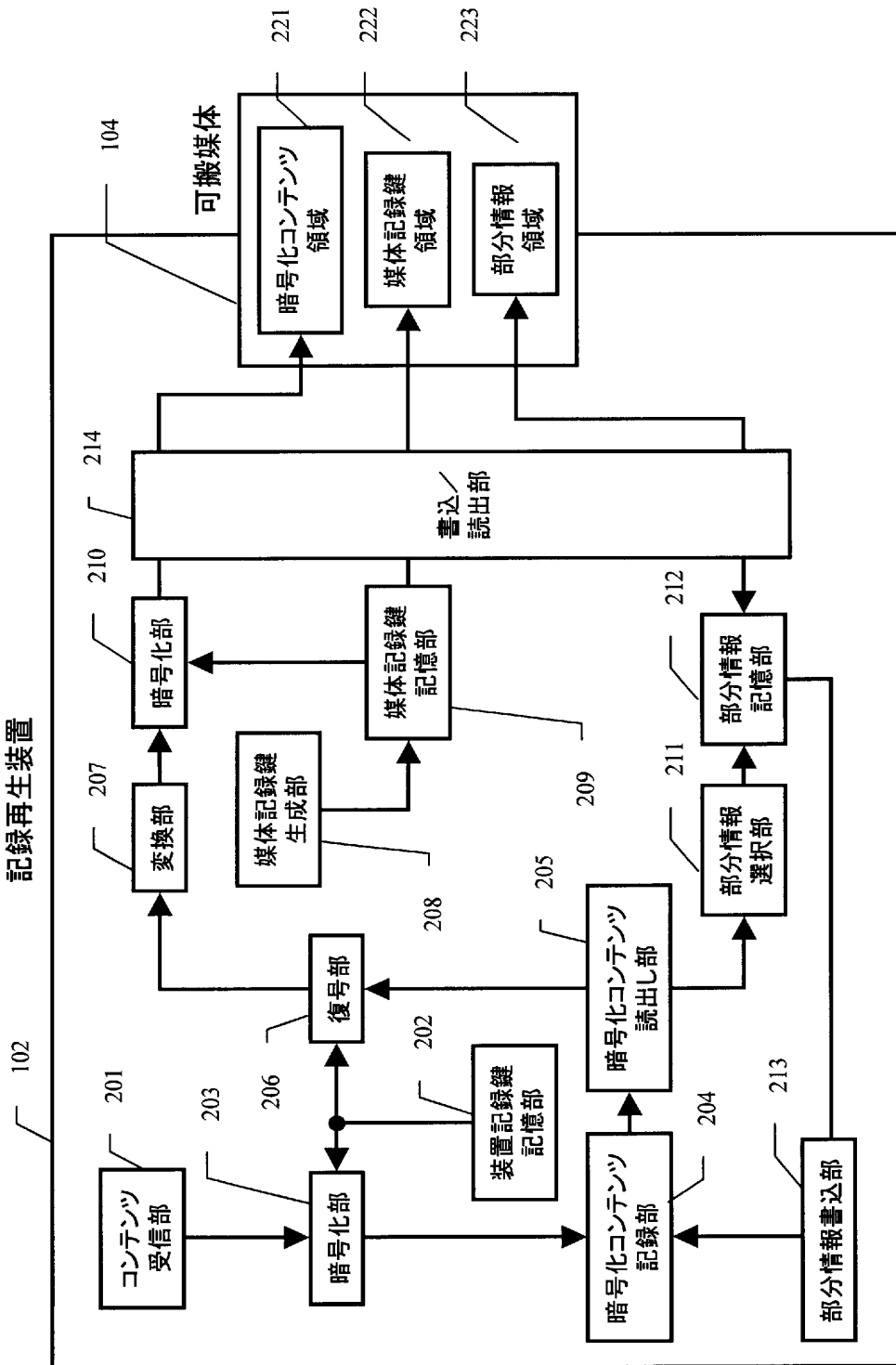
#### 【符号の説明】

【0074】

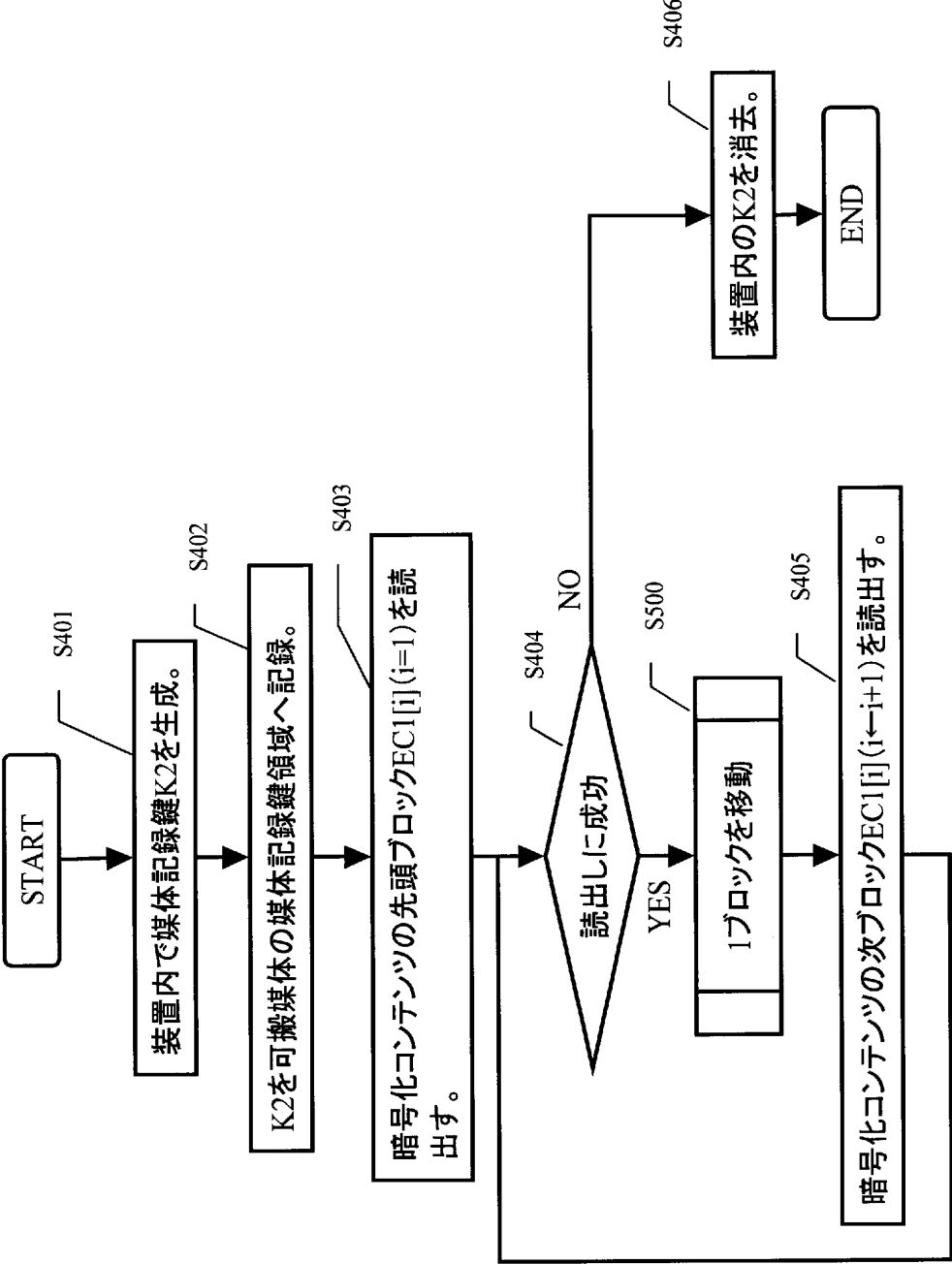
- 101 コンテンツ供給装置
- 102 記録再生装置
- 103 記録再生装置
- 104 可搬媒体
- 201 コンテンツ受信部
- 202 装置記録鍵記憶部
- 203、210 暗号化部
- 204 暗号化コンテンツ記録部
- 205 暗号化コンテンツ読出し部
- 206 復号部
- 207 変換部
- 208 媒体記録鍵生成部
- 209 媒体記録鍵記憶部
- 211 部分情報選択部
- 212 部分情報記憶部
- 213 部分情報書込部
- 214 書込読出部
- 801 暗復号化部

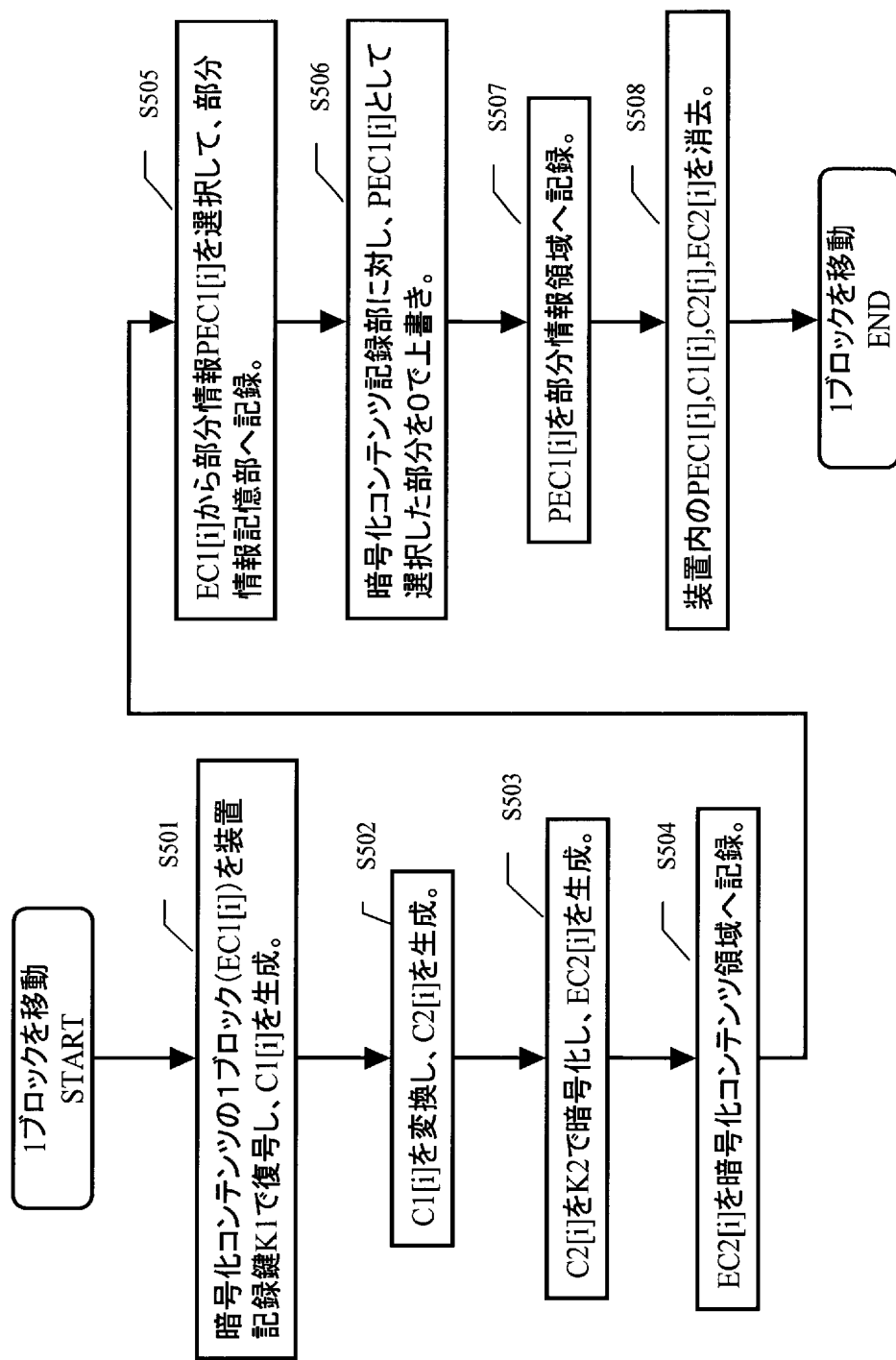


記録再生装置



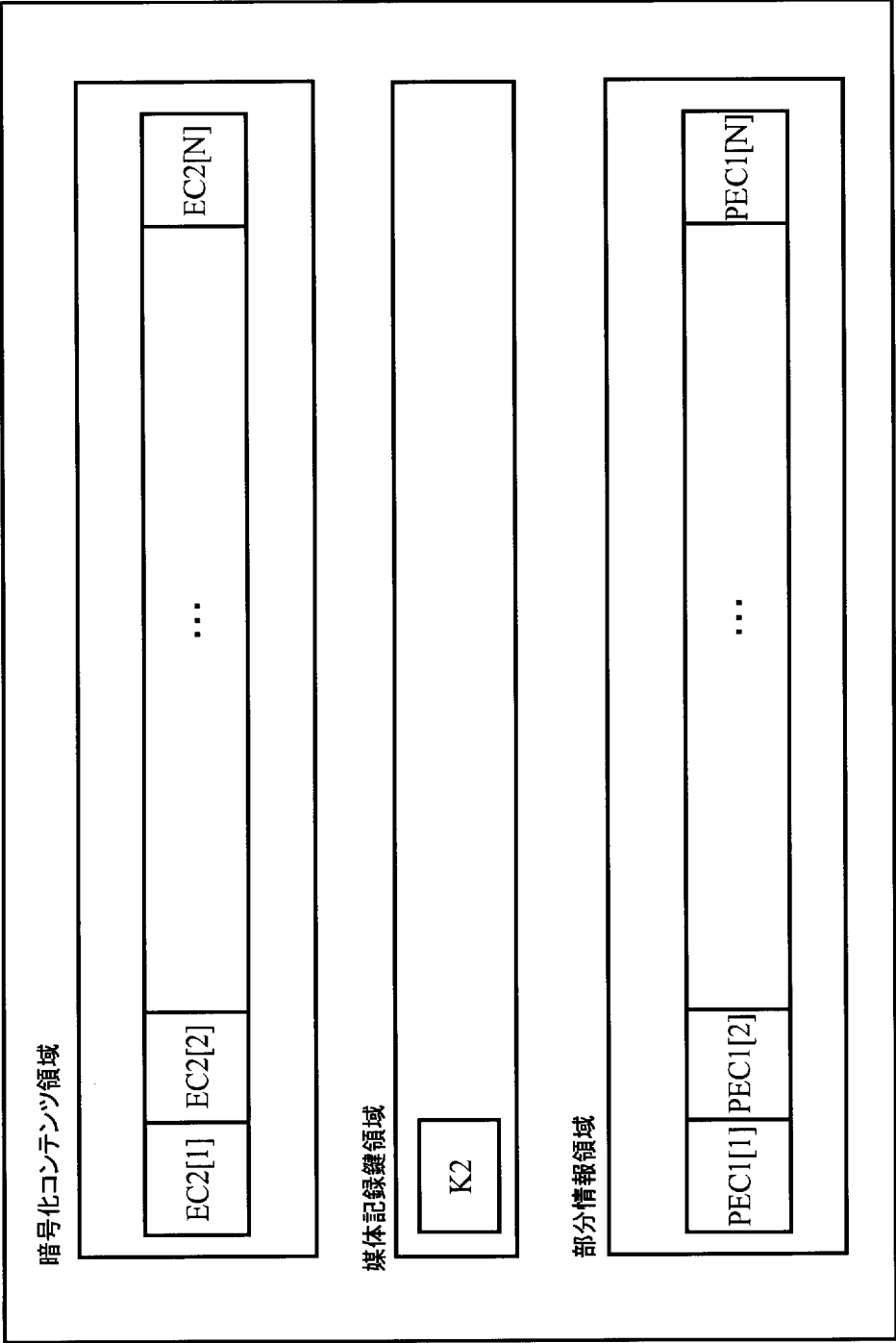
EC1[1]	EC1[2]	...	EC1[N]
--------	--------	-----	--------

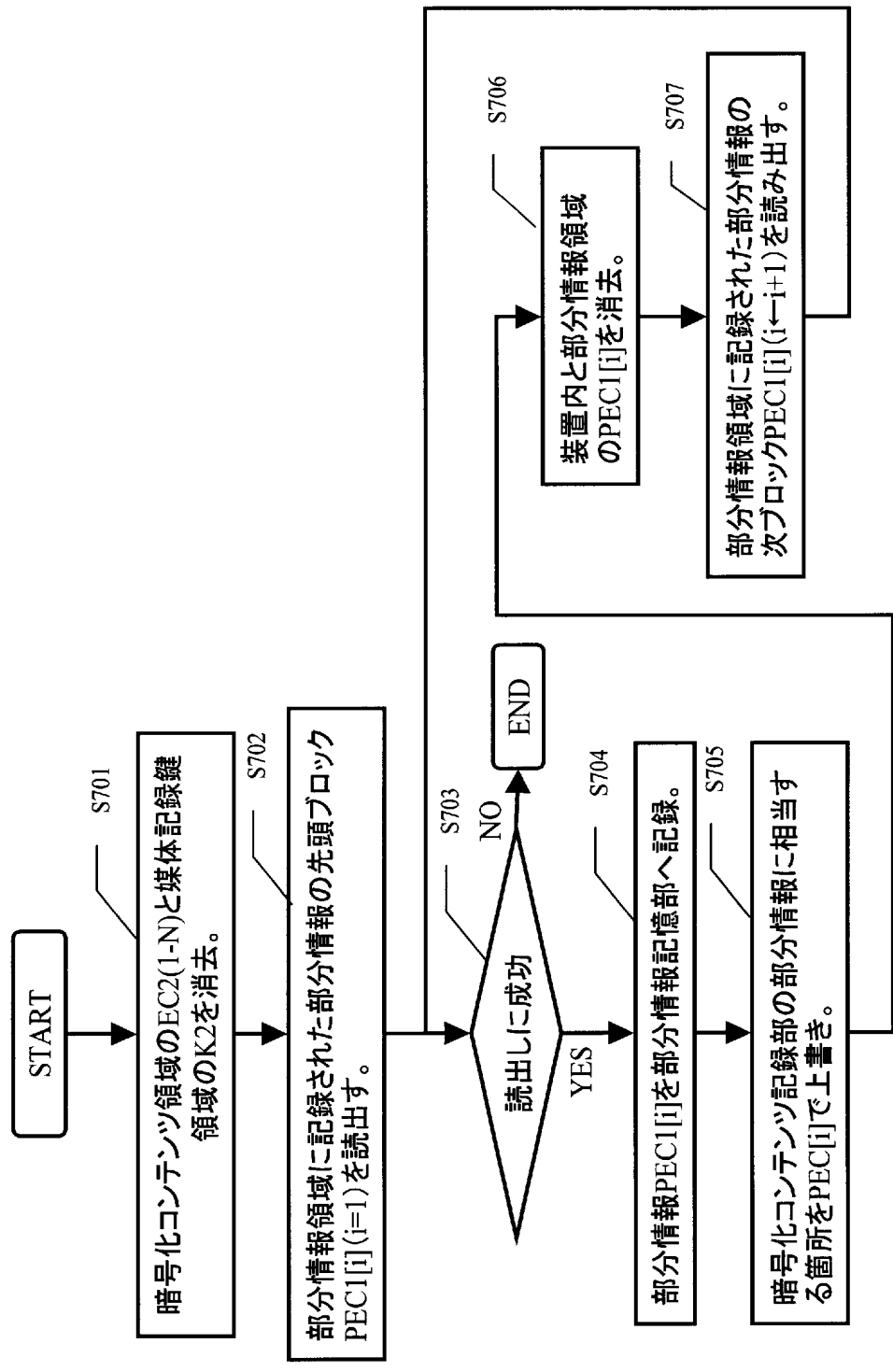




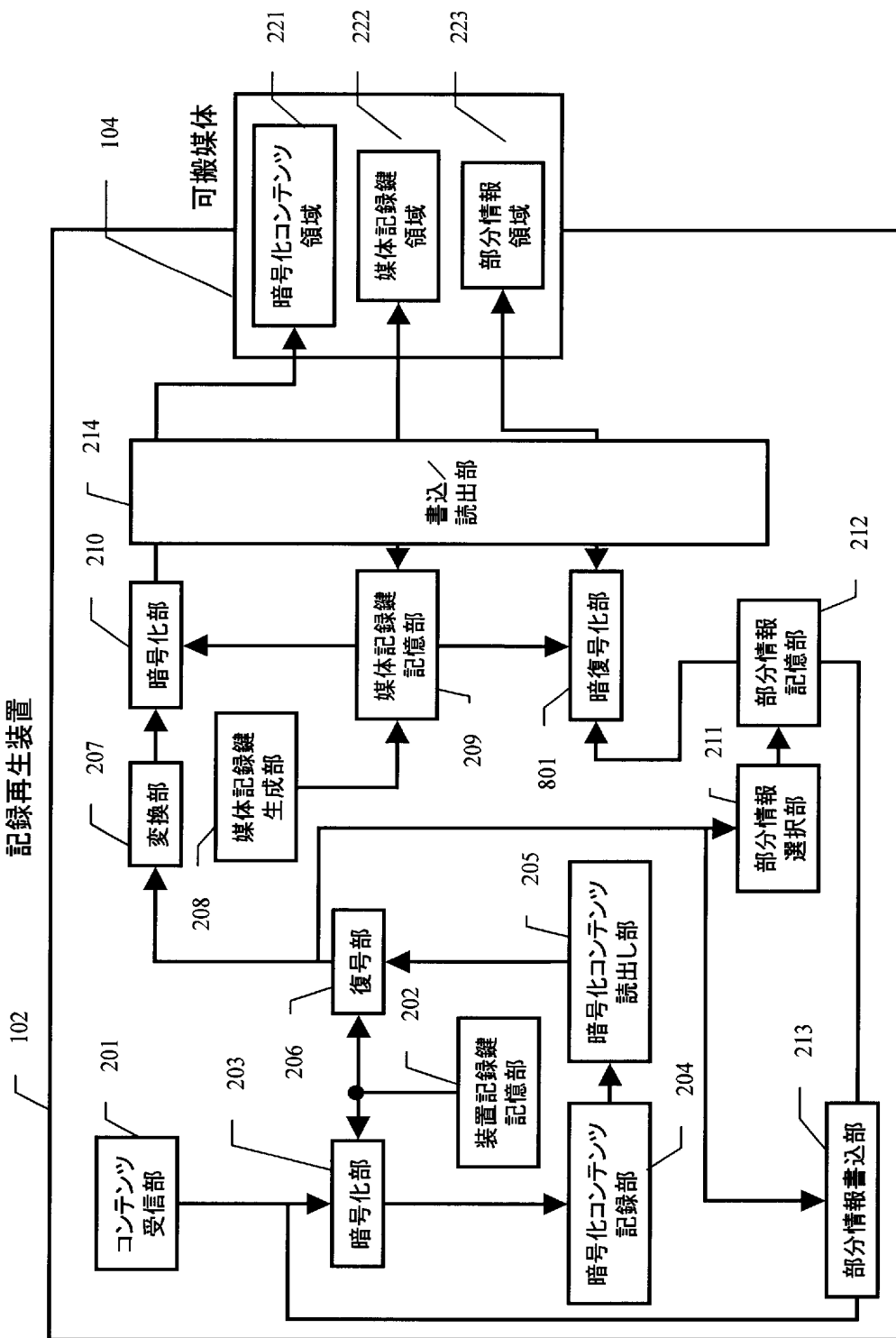


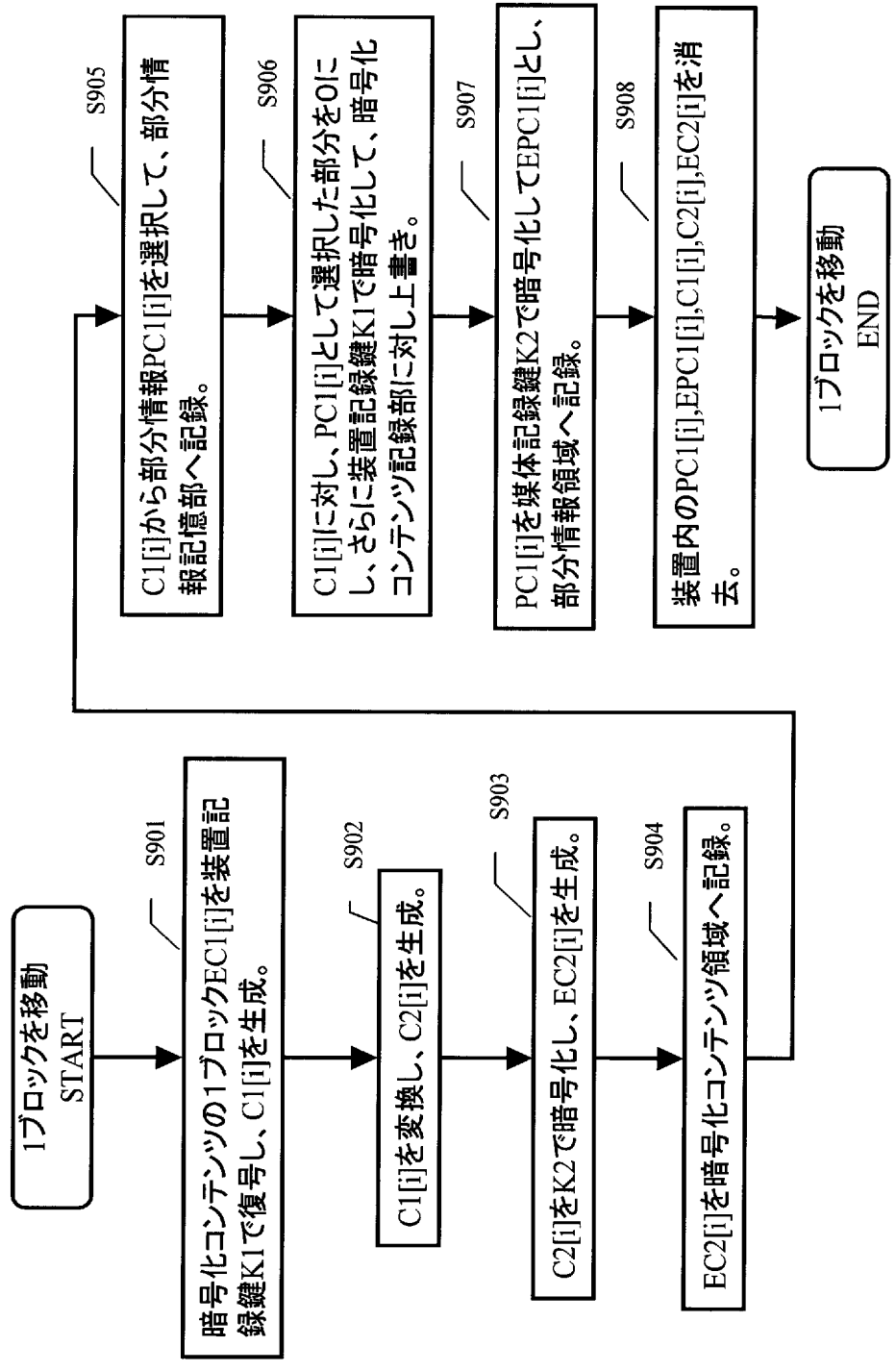
可搬媒体



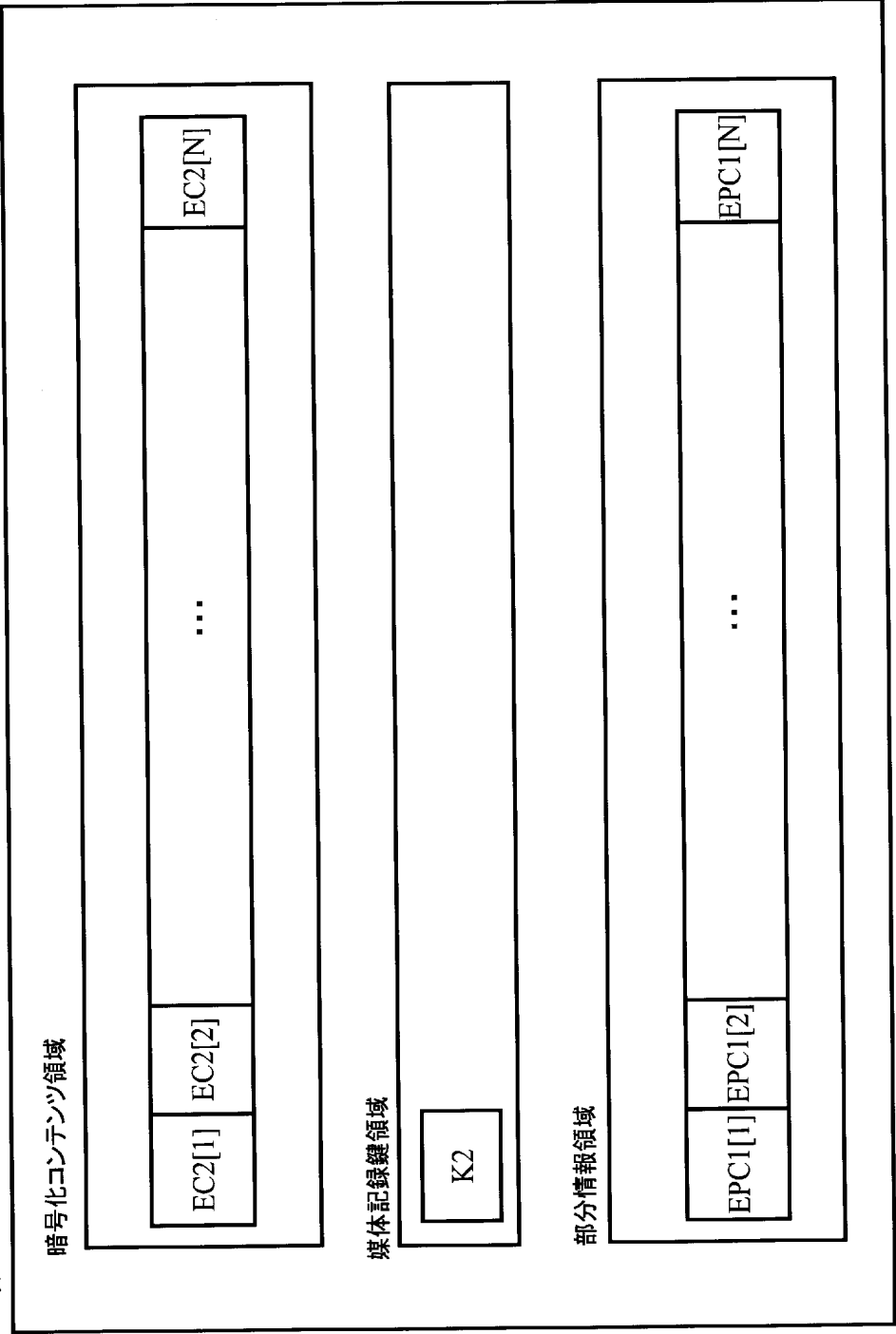


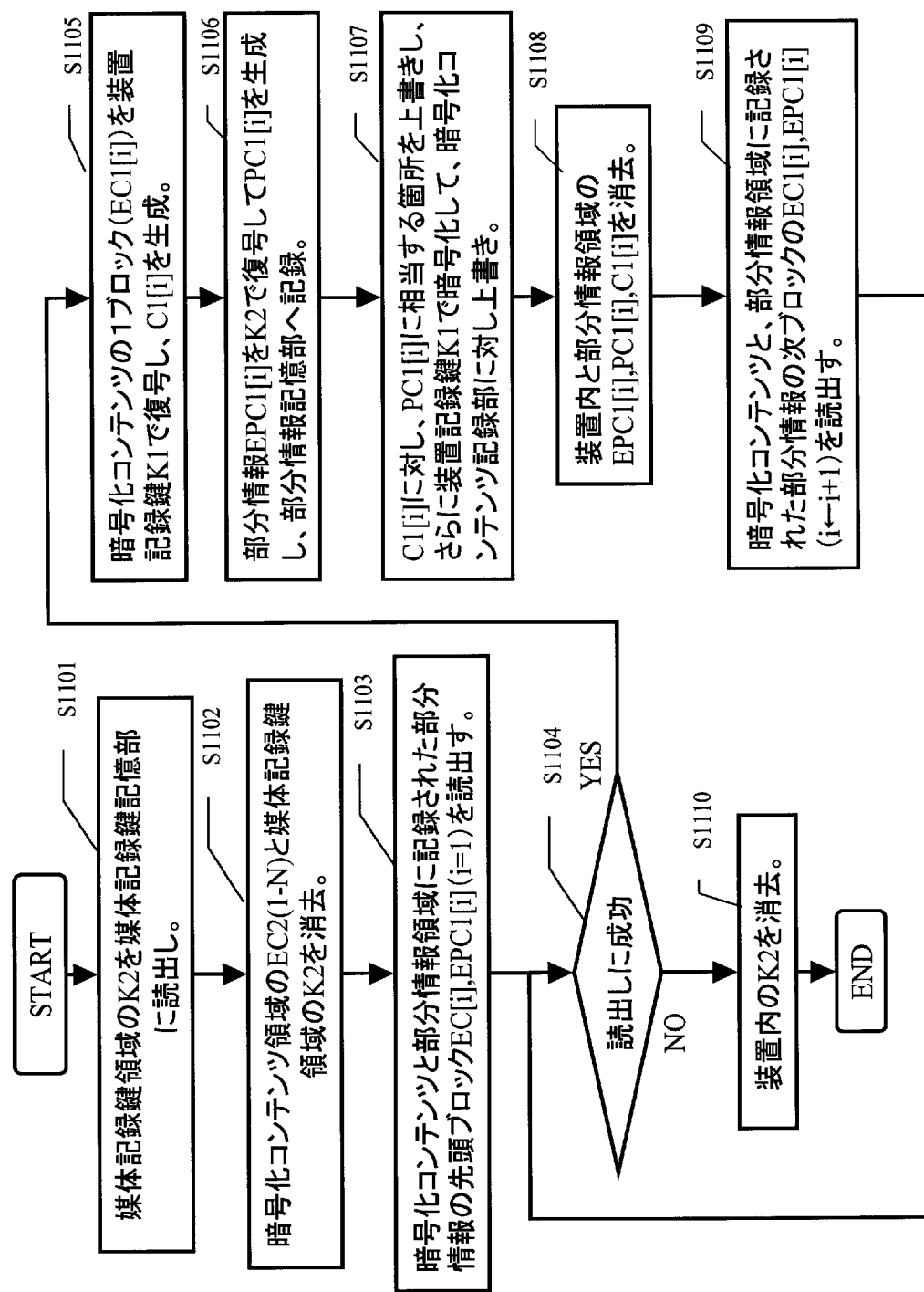
記録再生装置



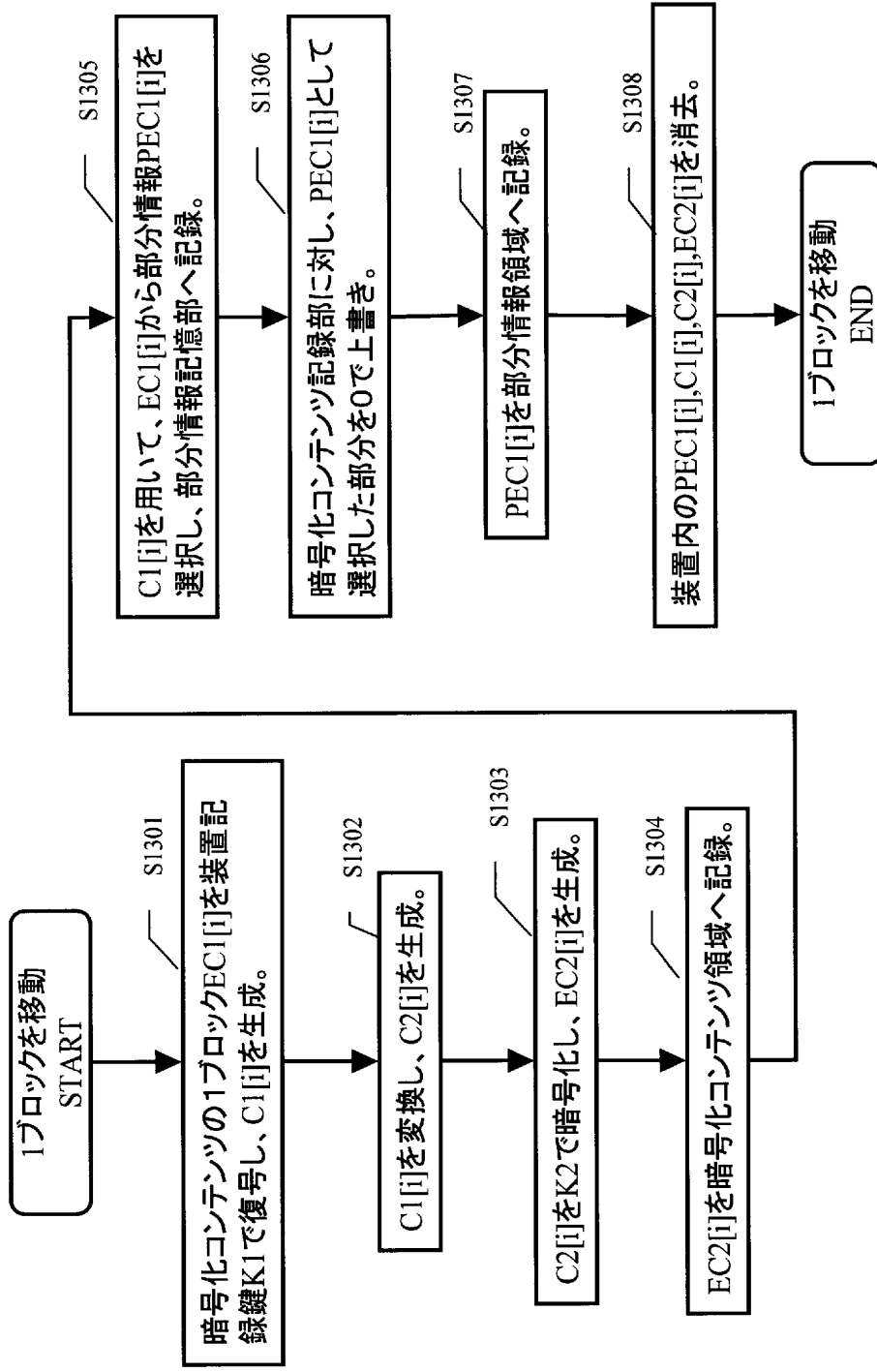


可搬媒体











【書類名】 要約書

【要約】

【課題】 移動元のコンテンツが高画質コンテンツであり、その画質を劣化させるなどしてサイズを小さく圧縮変換してからコンテンツの移動を行った場合、圧縮変換されたコンテンツだけがユーザの下に残り、高画質コンテンツが失われてしまう。

【解決手段】 コンテンツの移動時に当該コンテンツの部分情報を移動させることにより、記録再生装置内のコンテンツの全てを消去せずに利用不可状態にすることで、移動したコンテンツを再び戻す場合に、前記部分情報を移動させることにより、元々の高画質コンテンツを利用可能にする。

【選択図】 図 1

## 出願人履歴

0 0 0 0 0 5 8 2 1

19900828

新規登録

大阪府門真市大字門真 1 0 0 6 番地

松下電器産業株式会社